

**AFFIDAVIT**

I, Pepper M. Daigler, depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I am a Special Agent of the Federal Bureau of Investigation (“FBI”). I have been employed by the FBI since January 2016. I am currently assigned to the FBI Boston Division’s Providence Resident Agency. I am responsible for investigating Public Corruption, Civil Rights Violations and White-Collar crimes in Rhode Island. Previously, I was assigned to the Boston Field Office’s Healthcare Fraud Squad. I have experience investigating narcotics, money laundering, wire fraud, mail fraud and other crimes. My investigations have involved the use of surveillance techniques, and the execution of search, seizure, and arrest warrants.
2. I submit this affidavit in support of an arrest warrant and complaint charging RACHON WAITE, DOB: [REDACTED], last known address of [REDACTED], [REDACTED] with 18 U.S.C. § 1343 (wire fraud), 18 U.S.C. § 1344 (bank fraud), 18 U.S.C. § 1029 (access device fraud), and 18 U.S.C. § 1028A (aggravated identify theft) (the “Specified Federal Offenses”).
3. I also submit this affidavit in support of Applications for Search Warrants pursuant to Rule 41 of the Federal Rules of Criminal Procedure for a search of the following location and person:
  - a. the person of RACHON WAITE, DOB [REDACTED] (the “SUBJECT PERSON”), as more particularly described in Attachment A-1 for the items described in Attachment B-1, at whatever location he is found, regardless of WAITE’s location or proximity to SUBJECT PREMISES, including any cellular telephones or digital storage devices he may have on his person; and
  - b. the premises at [REDACTED] Veazie Street, [REDACTED] Providence, Rhode Island (the “SUBJECT PREMISES”), described in Attachment A-2, as more particularly described in Attachment A-2 for the items described in Attachment B-2;

4. As set forth below, there is probable cause to believe that located within the SUBJECT PREMISES, on and with the SUBJECT PERSON are evidence, fruits, and instrumentalities of violations the Specified Federal Offenses.
5. The facts in this affidavit come from my involvement in a collaborative investigation being handled primarily by the FBI, and Bristol Police Department in Bristol, Rhode Island. This affidavit is intended to show there is probable cause for the requested warrants and does not set forth all of my knowledge about this matter.

### **PROBABLE CAUSE**

#### **A. Overview**

6. From a date unknown, but not later than December 2020 through June 2021, WAITE has engaged in a fraud scheme, whereby he recruits persons via social media to provide him with their debit cards and personal identifying number (PIN) number for their debit cards and/or access to their bank accounts, for deposit of a check, with the expectation that after the check clears, WAITE will give them a portion of the check proceeds. The investigation has shown that WAITE has been using the bank accounts of these third parties to cash fraudulent checks, which are created using real account information of the victim company but which list a payee recruited by WAITE.<sup>1</sup> In the scheme, WAITE, himself or using the third parties, withdraws funds from the bank accounts into which the fraudulent checks were deposited, before the fraudulent nature of the check is deposited. As discussed herein, WAITE appears to have continued to engage in this fraudulent scheme through at least June 2021, based on his social media stories.

#### **B. Reports of Fraudulent Checks and Identification of Accounts Used by WAITE for Fraud Scheme**

*WAITE Uses CP's Bank Account for a Fraudulent Check Deposit for a Bristol, RI Business*

7. In March 2021, P [REDACTED] F [REDACTED], co-owner of MF Engineering Co. Inc. ("MF Engineering"), in Bristol, Rhode Island, reported to the Bristol Police Department that a fraudulent check

---

<sup>1</sup> The investigation has not yet identified the source of the checks – whether checks were stolen from mail and "washed" to change the payee, or if the account information was obtained and checks were created using that information.

in the amount of \$23,754.86 had been cashed on their business account. Bank records show that the fraudulent check was payable to C.P. and was deposited into the Citizen's bank account of CP.,<sup>2</sup> a resident of Coventry, Rhode Island.

8. Law enforcement agents spoke with CP in March 2021 and in May 2021 regarding the fraudulent MF Engineering check deposited into his Citizens Bank account. CP stated that his friend, SKS,<sup>3</sup> shared a story on social media about making money and then put CP in contact with Snapchat user: [REDACTED] isom. According to CP, CP asked SKS what RJ's story was all about and if getting money through RJ was true. According to CP, SKS told CP that she had heard about it from SF of West Warwick<sup>4</sup> (a friend of SKS's) and that CP should try it. I note, as discussed below, SKS reported that she told CP not to do the transaction with RJ. During the interview, CP showed law enforcement agents a picture on his phone with a Snapchat account for [REDACTED] isom, which had money bag emojis around the username.
9. CP told agents that he needed to make money at that time. CP said that he initiated contact with Snapchat user "[REDACTED] isom," who he later came to know him as "RJ." According to CP, RJ and CP communicated via Snapchat and via text and telephone using a telephone number of [REDACTED]-0756 for WAITE ("RJ").<sup>5</sup> CP explained that he understood from the Instagram story, and from communicating with RJ, that RJ would deposit money into CP's bank account, and thereafter withdraw some of the money, leaving a portion for CP. As described below, RJ, has been identified as RACHON WAITE.
10. According to CP, CP met WAITE (RJ) at an address provided by WAITE ("RJ") in Providence, Rhode Island. CP described RJ as a black male, in his 30's, with short hair and a tattoo on his right hand. CP gave RJ his Citizens bank ATM card and personal identifying number ("PIN"), so, as discussed between them, WAITE (RJ) could deposit

---

<sup>2</sup> The initials CP refer to a person known as C [REDACTED] P [REDACTED]. Certain persons, including CP, will be referred to through this affidavit by their initials to protect their privacy.

<sup>3</sup> The initials SKS refer to a person known as S [REDACTED] K [REDACTED] S [REDACTED].

<sup>4</sup> The initials SF refer to a person known as S [REDACTED] (J [REDACTED]) F [REDACTED].

<sup>5</sup> CP said that when RJ called him from this telephone, the name "A [REDACTED] P [REDACTED]" appeared on his phone. From our investigation, I believe that A [REDACTED] P [REDACTED] is WAITE's girlfriend and lives with him at the SUBJECT PREMISES.

money into CP's bank account. WAITE (RJ) told CP that CP would see money in his account soon and once the money was in CP's account, he and WAITE (RJ) would meet up again so CP could withdraw the money, and give it to WAITE (RJ). WAITE (RJ) told CP that they would both receive money from this withdrawal. RJ never told P [REDACTED] where the money came from.

11. On or about March 19, 2021, WAITE (RJ) told CP that the money, was in CP's bank account. CP checked his balance and saw that \$24,000 was on hold. He sent WAITE (RJ) a screen shot of the balance, and asked him to leave money that was needed for scheduled automatic withdrawals. CP later saw that his bank account was in the negative for approximately \$24,000, and send a screen shot of the balance to WAITE (RJ). WAITE (RJ) told CP that his bank account would go back to normal tomorrow.
12. Citizen's bank closed CP's account and kept the remaining funds, from CP's recent paycheck, as well. CP never saw WAITE (RJ) again, and WAITE (RJ) never returned CP's debit card.

*WAITE Uses SKS' and DF's Bank Accounts for Fraudulent Check Deposits  
for a Wrentham, MA Business*

13. On March 3, 2021, the Manager of Helping Hands of American Foundation, Inc. (Helping Hands) contacted the Wrentham, Massachusetts Police Department and reported that two fraudulent checks had been cashed against the Helping Hands bank account.
14. Information provided by Citizen's Bank showed that
  - on March 10, 2021, Helping Hands check number 9731, in the amount of \$7,417.41, bearing the name of SKS, of Coventry, Rhode Island, was deposited in person by a male at the Citizen's Bank branch located in Warwick, Rhode Island.
  - on March 15, 2021, Helping Hands check number 9617, in the amount of \$7,117.4, bearing the name of DF,<sup>6</sup> of Johnston, Rhode Island, was deposited into a Bank of America ATM.

---

<sup>6</sup> The initials DF refer to a person known as D [REDACTED] F [REDACTED].

*SKS Met WAITE on Snapchat and He Used Her Bank Account*

15. SKS, of Coventry, Rhode Island, was interviewed on May 12, 2001 regarding the fraudulent check deposited into her Citizen's Bank account. SKS told Agents that she met a person she knew as RJ on Snapchat in early 2021.<sup>7</sup> SKS said she didn't know if RJ was his real name. RJ, who has been identified as WAITE, asked SKS, via Snapchat, if she wanted to make money and told SKS that she would be helping people. WAITE (RJ) told SKS that he would take her ATM card and put money in her bank account. WAITE (RJ) told SKS that the proceeds of the check put in her bank account would be given to her and the charity.
16. SKS said that she met WAITE (RJ) at her father's house in West Warwick, Rhode Island. SKS gave WAITE her Citizen's Bank ATM card. SKS described WAITE (RJ) as a light skinned black male, approximately 30 years old, thin build, with a beard. WAITE (RJ) told SKS that he was from Providence, Rhode Island. When they first met, SKS gave WAITE (RJ) her ATM card so he could deposit a check into her checking account.
17. On March 10, 2021, WAITE (RJ) sent a photo to SKS, via Snapchat, of a Citizen's Bank deposit slip indicating that a deposit of \$7,417.41 had been made into her Citizen's Bank account on March 10, 2021. SKS never saw the check that WAITE (RJ) deposited into her account. Citizen's Bank surveillance footage of the deposit shows a black male, wearing a Yankees hat, mask, black coat and dark colored shirt making the deposit via a teller. The Yankees hat in the Citizen's Bank surveillance footage is appears similar to a Yankees hat worn by WAITE in a photo posted on his Instagram account. SKS viewed still photos from the surveillance footage and identified the man as RJ.
18. SKS said that WAITE (RJ) offered to pay SKS for making referrals or recruit other people to make the same type of transaction. SKS told WAITE (RJ) told RJ that she would refer people to him and that she would post something on her Instagram story. SKS said that she posted on Instagram for him just to be nice and did not accept any

---

<sup>7</sup> SKS showed agents her phone and S [REDACTED] showed agents her phone and Snapchat account, and an account name for [REDACTED] ison [sic].



- money. SKS said that she learned about WAITE (RJ) from her friend SF<sup>8</sup> of West Warwick via Instagram. SKS said that SF told her that working with RJ was not a scam.
19. A few days later, SKS met WAITE (RJ) and they went to Citizen's Bank in Coventry, RI to withdraw the money from her account. SKS withdrew \$7,000. WAITE kept \$5,000 and SKS kept \$2,000. Shortly after SKS made the withdrawal she checked her bank account and saw that the account had a negative balance. SKS sent WAITE (RJ) a message via Snapchat and a text message, via [REDACTED], about the negative balance. SKS asked WAITE (RJ) if he had done something to her account. Thereafter, WAITE (RJ) blocked SKS on Snapchat.
20. During her interview, when SKS was asked if she knew others who had done this sort of activity with WAITE, she initially said no, but when asked about CP, she said she told him not to do a transaction with RJ. As described above, CP told agents that SKS had told him about WAITE (RJ) and that he should try it.

*DF Met WAITE on Snapchat and WAITE Used His Bank Account*

21. DF, of Johnston, Rhode Island, was interviewed on June 1, 2021 regarding the fraudulent Helping Hands check deposited into his account. DF told Agents that he met WAITE, via Snapchat, in March 2021. DF said that Snapchat user [REDACTED] isom appeared as a "quick add" in his Snapchat account, and that he and [REDACTED] isom had mutual friends.
22. Snapchat user [REDACTED] Isom asked DF if he wanted to make some quick money. At the time, DS did not have a job and needed the money. WAITE met DF at his house in Johnston, Rhode Island. DF described WAITE as a black male, with a beard, and tattoos on his arms. DF stated that WAITE had a Glock 19 in his waistband when they met.
23. WAITE told DS he was going to deposit two checks into DF's Bank of America account. WAITE told DF that they would split the processed 75/25; with 25% going to DF. DF did not know where the checks came from, but now realizes that the checks were fraudulent.
24. DF gave WAITE his Bank of America ATM card, PIN number, account number and routing number for WAITE to deposit the checks. WAITE called DF, via [REDACTED]-0756,

---

<sup>8</sup> The initials SF refer to a person known as S [REDACTED] (J [REDACTED]) F [REDACTED]. She will be referred to by her initials through this affidavit, to protect her privacy.

and told DF to check his bank account to see if the funds were in the account. DF checked his account and saw that the deposited check had bounced. WAITE asked DF if he wanted to try to deposit another check and DF declined. DF had no further contact with WAITE and did not get his debit card back from WAITE.

25. DF told agents that he is still friends on Snapchat with WAITE and showed agents a current Snapchat image from WAITE's account that stated: "Tap in if u tryna make a few bands easy." Based on my experience "bands" refers to cash and the bands banks place around large amounts of cash. DF stated that this was an advertisement by WAITE. Based on viewing this Snapchat image, I believe that WAITE was continuing with this conduct through at least the date of DF's interview.
26. During the June 1, 2021 interview, DF also showed agents a screen shot of a Snapchat post by WAITE that appeared to show a submitted Paycheck Protection loan application. The screen shot stated "Ralph, your PPP loan application has been submitted." From my review of the Small Business Administration website, I am aware that the Paycheck Protection Program (PPP) was a loan offered through the Small Business Administration for businesses impacted by COVID-19 and that it expired as of May 31, 2021. Based on my viewing of the image shown by DF relating to the PPP loan, it appears that WAITE submitted at least one PPP loan in the name of a third party and was sharing this information with others on social media, similar to the manner in which he recruited others for the fraudulent check through the expiration date of the PPP program.

C. State Search Warrant for Snapchat Account Identifies WAITE and Additional Offense Conduct

*Identification of RACHON WAITE as Snapchat User [REDACTED]isom*

27. On or about March 31, 2021, the Bristol Police Department executed a Rhode Island state search warrant on Snapchat for content related to username: [REDACTED]isom. In response to the state search warrant, Snapchat provided subscriber information, discussed above, chat content, chat media, photos, video and auto recordings, a friend's list and IP data from March 30, 2020 through March 31, 2021.
28. The Snapchat Account Information provided for [REDACTED]isom listed the user of that ID as: "[REDACTED]isom." The email address associated with the account was [REDACTED]isom [REDACTED]

and phone number associated with the account [REDACTED]. Snapchat also records show that the user of [REDACTED] isom listed [REDACTED], the SUBJECT PREMISES, as a shipping address to a user on Snapchat for the purchase of products.

29. The Snapchat response contained a photo that was an invitation for “Rachon’s 30<sup>th</sup> Birthday: [REDACTED]; 8PM Onwards; [REDACTED]. The invitation also contained a photo of a light skinned, black male, with a beard, and a tattoo on his right forearm.
30. In messages provided by Snapchat, the user of the account provided the following Instagram username -- [REDACTED] lane27 -- to individuals he communicated with.
31. A review of the public Instagram profile for [REDACTED] lane27 on May 7, 2021 showed several photos of a light skinned black male with facial hair. In the photos, tattoos are visible on the inside of his left and right forearms and the top of his right hand. In one photo, the man pictured is seen wearing a gold chain and pendants and a gold bracelet on his right hand. On the public profile, the user of [REDACTED] lane27 wrote/posted that his Snapchat username is: [REDACTED] isom. The user also wrote/posted “R.I.P. G [REDACTED] I [REDACTED]” A December 12, 2020, WPRI.com article stated that G [REDACTED] I [REDACTED] was killed by a hit and run driver in December 2008 in Providence, Rhode Island. The article contained the following statement: “G [REDACTED] [REDACTED], [REDACTED] WAITE, was just 18 when she died.”
32. Documents from Rhode Island Department of Corrections identify as Rachon L WAITE, with a DOB: [REDACTED], phone number [REDACTED]-0756, and address of [REDACTED], the SUBJECT PREMISES.<sup>9</sup>
33. Photos from the Snapchat photo invitation, and the public profile of [REDACTED] lane27 are both visual similar to the photo provided by the Rhode Island Department of Corrections for Rachon WAITE. Based on my review of these records, I believe they depict the same individual.

---

<sup>9</sup> According to criminal history records, Waite was incarcerated by the Rhode Island Department of Corrections for 2nd Degree Burglary from January [REDACTED] through May [REDACTED].



*Snapchat Records Reveals Additional Fraudulent Check Activity.*

34. A review of the Snapchat records showed that WAITE deposited checks from the Varma Group and Amica Mutual Insurance, both of which have been determined to be fraudulent.
35. Agents have interviewed T [REDACTED] V [REDACTED], owner, Varma Group LLC in East Amherst, New York on May 26, 2021. Varma told investigators that her company was victim of a fraud. Varma reviewed a copy of the fraudulent check. Varma stated she never issued a check to JV and confirmed that it was not her signature on the company check.

*JV Met WAITE on Snapchat and WAITE Used His Bank Account*

36. The Snapchat records showed the WAITE exchanged messages with Snapchat user J [REDACTED] [REDACTED] regarding fraud check activity. In one of these messages, a screen shot showed the name JV<sup>10</sup> on a banking transaction. Snapchat user J [REDACTED] [REDACTED] was identified as JV of West Warwick, Rhode Island.
37. JV was interviewed by law enforcement agents on May 25, 2021. JV stated that he saw a story on a friend's Snapchat page with a man advertising about a way to make money. JV asked his friend if that story was real and if he could make some money. The friend told JV to contact "RJ" via Snapchat username: [REDACTED] isom. JV confirmed that his Snapchat username was J [REDACTED] [REDACTED].
38. WAITE (RJ) and JV initially communicated via Snapchat. WAITE (RJ) told JV that he had a check from Varma Group, LLC that WAITE needed cashed. WAITE told JV the check was from stock trading. WAITE (RJ) told JV the he needed his bank account number, routing number and debit card. WAITE (RJ) told JV that he would deposit the check into his bank account, then they would meet up when the check cleared and withdraw the money, and he and JV would split the money 50/50. WAITE (RJ) told JV the amount of money received by individuals varied from \$600 to \$10,000.
39. After their Snapchat communications, JV met WAITE (RJ) at the Lowes parking lot in Warwick, Rhode Island. JV described WAITE (RJ) as a thin, black male, with facial hair

---

<sup>10</sup> The initials JV refer to a person known as J [REDACTED] V [REDACTED].

and a tattoo on his arm or wrist. JV gave WAITE his Centerville Bank debit card and pin to deposit the check.

40. When JV checked his bank account a few days after meeting with WAITE (RJ), he saw that the check had been deposited.
41. WAITE (RJ) contacted JV and told him to go to Centerville Bank and withdraw \$6,000. JV was only able to get \$3,000 or \$4,000 out of the ATM. WAITE (RJ) directed JV to go to the Centerville Bank's West Warwick branch and take out the rest of the money. JV took out the money as directed and met WAITE (RJ) at the CVS in West Warwick, Rhode Island. JV thought he and WAITE (RJ) were going to split the money 50/50, but WAITE (RJ) told JV that he had to give money to the individual who drove WAITE to the location. WAITE (RJ) gave JV \$2,000. WAITE (RJ) asked JV if he wanted to deposit checks again and JV stated that he did, and WAITE kept his Centerville Bank debit card. WAITE (RJ) also told JV to post an advertisement on his Snapchat stories and WAITE (RJ) would pay him a \$100 bonus for each person he referred.
42. The day after he withdrew the money, JV received a call from Centerville Bank telling him that the deposited check had bounced. JV contacted WAITE (RJ) via Snapchat. WAITE (RJ) told JV that he was surprised and told JV to get a new bank account.
43. JV contacted WAITE (RJ) again when he saw that additional money, his tax refund and employment bonuses, had been withdrawn from his account. JV sent WAITE (RJ) screenshots of his Centerville Bank account via Snapchat. JV later learned that the money had been withdrawn from a Santander Bank ATM. JV tried to get the Santander Bank ATM withdrawal reversed, but the bank closed his account.
44. JV also said that a woman had messaged him on Facebook stating that she found his debit card on the ground in Providence, Rhode Island. She said she would mail it to him, and JV received the card in the mail. When JV asked WAITE (RJ) about the debit card, WAITE (RJ) told JV that he still had the debit card.
45. Surveillance footage provided by Centerville Bank for the date and time the Varma Group LLC check was deposited into JV's account shows a Black SUV arrive in the Centerville Bank parking lot. An individual wearing black sneakers, light colored pants, white shirt, light colored baseball hat, and zipped dark campo style coat exited the vehicle and entered that ATM vestibule. The individual conducted the transaction at the ATM

whole holding their cell phone in a dark colored case. During the transaction a tattoo is seen on the top of the individual's right hand and a gold bracelet is seen on the individual's right wrist. Based on my review of the surveillance footage, I believe that the tattoo visible is consistent with pictures in WAITE's Instagram account showing his tattoo on his hand.

*TRR Met WAITE on Snapchat and WAITE Used Her Bank Account*

46. Records from WAITE's Snapchat account included an image that showed Santander Bank debit card in the name of TRR<sup>11</sup> on top of a December 22, 2020, Santander deposit slip showing an account balance was \$15,478.42
47. TRR, of Cranston, Rhode Island, was interviewed by law enforcement agents on May 19, 2021 relating to the image found in WAITE's Snapchat return. TRR stated that she met WAITE in December 2020 through Snapchat. TRR stated that she and WAITE were dating at the time. Initially, TRR stated that before Christmas 2020, she received a check in the mail from Amica, and had a friend deposit the check for her. TRR said that she thought the check was from an accident that occurred 14 years prior, and viewed the check as a "sign" to help her out around the holidays. She said she did think that the check looked "wonky" like a photograph.
48. TRR said that the friend who helped her was "Raj" or "Ra," who she described as a light skinned black male, approximately early to mid-30s, with a beard, and tattoos on his arm. She said they met on an online dating website and dated for a few weeks. She said his Instagram account was [REDACTED] lane and she thought "[REDACTED] Isom" or something with "Junior" in it might be his real name.
49. When agents showed TRR an image of a Snapchat account with the user account, tao2style, in which she was sending her full name and address. TRR said that was her account and that she sent WAITE her full name and address so he knew where to meet here. TRR was also asked about an image in which WAITE sent her a picture of her Santander bank account statement and debit card. TRR also said that the day that the

---

<sup>11</sup> The initials TRR refer to a person known as T [REDACTED] R [REDACTED] R [REDACTED]. She will be referred to by her initials through this affidavit, to protect her privacy.

check was deposited, she sent her PIN number to “R[REDACTED]” so he could deposit the check for her. TRR told agents that “R[REDACTED]” said he knew someone at Amica. TRR said she didn’t know why he would send her a picture of her Santander statement and bank card.

50. After agents reminded TRR of the need to be truthful, TRR said that WAITE (R[REDACTED]) acquired a check from Amica Mutual Insurance. WAITE (R[REDACTED]) told TRR that his bank account was not in good standing and that he needed to deposit the check into her bank account. WAITE (R[REDACTED]) told TRR that he had been doing “this,” meaning falsified checks, for a while. WAITE (R[REDACTED]) told TRR to put her name and address on the check. TRR gave WAITE (R[REDACTED]) her Santander debit card and her ATM pin to deposit the check. WAITE (R[REDACTED]) kept TRR’s debit card and told TRR that he would make sure the check cleared. TRR never saw the physical check but saw a copy of the check online.
51. TRR went to Santander Bank to withdraw the money and met WAITE (R[REDACTED]) at a 7-11 in Cranston, Rhode Island. WAITE (R[REDACTED]) told TRR that he was going to give TRR money, but that he needed to talk to the person at Amica that he got the check from first. TRR said that she never received any money from WAITE (R[REDACTED]).
52. WAITE (R[REDACTED]) told TRR that if she posted information about the transaction, he would give her money for anyone she recruited. TRR said that she posted for WAITE (R[REDACTED]) but never received any money.
53. Santander closed TRR’s account, after which TRR was in contact with WAITE (R[REDACTED]). TRR said that she has not seen or spoke to WAITE since early January 2021.

*Additional Evidence of Fraud by WAITE in Snapchat Records*

54. A review of the Snapchat photos and audio recordings included posts that appears to be WAITE was trying to solicit individuals to help him commit fraud.
  - a. On January 11, 2021, WAITE posted the following to his Snapchat story: “New Week New Money Hit Me And Cash Out.” The post also included the names of several banks and stated that “Negative Balances Can Still Do Under \$500.”
  - b. On March 9, 2021, WAITE posted the following to his Snapchat story: “Tap in easy money \$2-\$5k.” The post includes the name of three banks and “Credit Unions.” The post also stated “Next day availability. Negative balances excepted under- 500.”

55. As described above, SKS, DF, and TRR told agents that WAITE asked them to post advertisements on their Snapchat and offered to pay them for making referrals or recruiting other people to conduct the same transaction with him. Based on my training and experience, and interviews conducted during this investigation, I believe that WAITE used the above described advertisements to recruit and entice others to participate in his fraud scheme with the illusion they would earn cash quickly.

56. The review of Snapchat records also indicates that WAITE used Snapchat messages to explain the fraud scheme to users.

- a. On January 25, 2021, WAITE had the following exchange with user g [REDACTED] that he will use his/her first name, address and ATM card to deposit a check and that when the money becomes available they will meet at the bank to withdraw and split the funds.

From:	To:	Message:	Date:
WAITE	G [REDACTED]	So basically how it goes is I would just meet up with you get your info for like check like your first name address ect and also card for depositing and then once [it's] and and then becomes available [I'll] meet with u again and [we'll] go to the bank and [you'll] withdraw it and then [we'll] split it...	1/25/21

- b. On February 19, 2021, WAITE had the following exchange with user kr [REDACTED], that he would make a “regular deposit” into her account, and when the money was available in her account, he/she would split the money with WAITE. Kr [REDACTED] asked WAITE if the deposit is “a fake check?” WAITE responded that the check is official.

From:	To:	Message:	Date:
[REDACTED] isom	kr [REDACTED]	Basically, how it goes [It's] a regular deposit in your account and once the money is available you would just withdraw some and split it with me [that's]how it goes	2/9/21
kr [REDACTED]	[REDACTED] isom	A regular deposit of what? A fake check?	2/9/21
[REDACTED] isom	kr [REDACTED]	Regular deposit and no	2/9/21
[REDACTED] isom	kr [REDACTED]	[It's] official	2/9/21
kr [REDACTED]	[REDACTED] isom	Where does this deposit come from?	2/9/21



isom	kr	I do it	2/9/21
kr	isom	So what you need all my account info?	2/9/21
isom	kr	No just would be like your first and last name and address	2/9/21

- c. On March 5, 2021, WAITE had the following exchange with user tu as to whether he/she wanted to make money and stated that he/she can make “Easy money few thousand.” WAITE explained to tu that he/she needs a bank account, and when the money was available, he/she would withdraw the money.

<u>From:</u>	<u>To:</u>	<u>Message:</u>	<u>Date:</u>
isom	tu	U tryna make some money	3/5/21
isom	tu	Lmk	3/5/21
isom	tu	Easy money few thousand	3/5/21
tu	isom	Waddup	3/5/21
isom	tu	Just need an account to make the money	3/5/21
tu	isom	Okay how much	3/5/21
tu	isom	Send me details [it's] m down	3/5/21
isom	tu	Ok u would just need an account to get it I would simply deposit it into your account and once [it's] available [you'll] withdraw it and [we'll] split it up depending on how much goes in u can make a couple to a few thousand	3/5/21

57. WAITE's Snapchat account contained approximately two dozen photographs of deposits slips from various banks with unique account numbers. The response from Snapchat also included voice recordings that appear to be recordings of WAITE described the fraudulent check scheme to others, and include information such as that WAITE will need bank account information that will be used to deposit a check

#### **EVIDENCE OBTAINED DURING RESIDENTIAL SEARCHES**

58. Based on my training and experience, I know that during the course of residential searches, I and other agents have also found items of personal property that tend to identify the person(s) in residence, occupancy, control, or ownership of the SUBJECT PREMISES and computer devices located therein. Such identification evidence is typical of the articles people commonly maintain in their residences, such as canceled mail,

deeds, leases, rental agreements, photographs, personal telephone books, diaries, utility and telephone bills, statements, identification documents, and keys.

59. Given the nature of this crime, I also believe it is reasonable to believe that the access devices, such as debit cards, checks, bank account information and information relating thereto (names, passwords, online user log ins, etc.) would be maintained a place that allowed for safe storage, but ready access, such as a residence, for creation of fraudulent checks and use for access to accounts.

#### **EVIDENCE RELATING TO FRAUD OFFENSES**

60. Based on my training and experience and familiarity with investigations into fraud conducted by other law enforcement agents, I know the following:

- a. Individuals maintain in their homes, both in paper and electronic format, among other items, records regarding the receipt and expenditure of money, documents relating to the purchase of assets, and records pertaining to their employment or business, even if that business is an illicit business.
- b. Given the nature of fraud, I believe that participants in a long running fraud that involves several participants, more often than not, will keep records containing names, addresses, email addresses, social media accounts, and telephone numbers of co-conspirators, as well as targets, victims, and those used to perpetrate the fraud, amounts received from them, and amounts sent to third parties. These records are necessary to further the illicit fraud business and can be found in paper form or stored electronically in cell phones and other electronic devices.
- c. I also know that those who make use of stolen personal identification as part of their fraud schemes, will often keep lists of the stolen PII, and notations on how and when that identify may be used, and any passwords for that "identity." I am also aware that fraudsters often maintain such documents related to their criminal activities at their residences or other locations over which they have control for an extended period of time, due to the high value associated with stolen PII that has been successfully used.
- d. From training and experience, I know that individuals who amass proceeds from illegal activities routinely attempt to further that conduct and/or conceal the

existence and source of their funds by engaging in financial transactions with domestic and foreign institutions, and others, through all manner of financial instruments, including cash, cashier's checks, credit and debit cards, money drafts, traveler's checks, wire transfers, etc. Records of such instruments, including ATM receipts, are oftentimes maintained at the individual's residence.

- e. There are many reasons why criminal offenders maintain evidence for long periods of time. First, to the offender, the evidence may seem innocuous at first glance (e.g. financial, credit card and banking documents, travel documents, receipts, documents reflecting purchases of assets, personal calendars, telephone and address directories, checkbooks, videotapes and photographs, utility records, ownership records, letters and notes, tax returns and financial records, escrow files, telephone bills, keys to safe deposit boxes, packaging materials, computer hardware and software). To law enforcement, however, such items may have significance and relevance when considered in light of other evidence. Second, the criminal offender may no longer realize he/she still possesses the evidence or may believe law enforcement could not obtain a search warrant to seize the evidence. The criminal offender may also be under the mistaken belief that he/she has deleted, hidden or further destroyed computer-related evidence, which in fact, may be retrievable by a trained forensic computer expert. Thus, records and ledger-type evidence that one would think a prudent person might destroy because of its incriminatory nature are sometimes still possessed months or even years after the records were created.
- f. Based on my knowledge with respect to facts and circumstances in this investigation, as well as my experience and training relating to cases involving individuals engaged in fraud schemes, as well as my discussions with other agents who investigated such cases, I know that it is a common practice for individuals engaged in these illegal activities to maintain the items and records or documents as set forth in Attachments B-1 through B-2, whether maintained on paper, in hand-written, typed, photocopied, or printed form, or electronically on a computer or cell phone, hard disks, external drives, RAM, flash memory, CD-ROMS,

memory sticks, USB drives, and other magnetic or optical media, or any other storage medium.

### **TRAINING AND EXPERIENCE ON DIGITAL DEVICES**

61. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:
- a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.
  - b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.
  - c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

- d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain “booby traps” that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.
62. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:
- a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.
  - b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.
63. The search warrant also requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:
- a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user’s fingers on a device’s fingerprint scanner for approximately one second. To unlock a device



enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

- b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.
- c. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress the user's thumb- and/or fingers on the device(s); and (2) hold the device(s) in front of the user's face with her eyes open to activate the facial-, iris-, and/or retina-recognition feature.
- d. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

#### **REQUEST FOR SEALING**

64. Because this investigation is continuing and disclosure of some of the details of this affidavit may cause the targets or other affiliated persons to flee or further mask their identity or activities, destroy physical and/or electronic evidence, or otherwise obstruct and seriously jeopardize this investigation, I respectfully request that this affidavit, and associated materials seeking this search warrant, be sealed until further order of this Court. Finally, I specifically request that the sealing order not prohibit information obtained from this warrant from being shared with other law enforcement and intelligence agencies.

**CONCLUSION**

65. For all of the reasons described above, there is probable cause to arrest RACHON WAITE for the Specified Federal Offenses and to believe that the items to be seized described in Attachment B-1 and B-2, will be found in a search of the SUBJECT PERSON and SUBJECT PREMISES described in Attachment A-1 and A-2.

Sworn to under the pains and penalties of perjury.

Respectfully submitted,

Pepper M. Daigler  
Special Agent

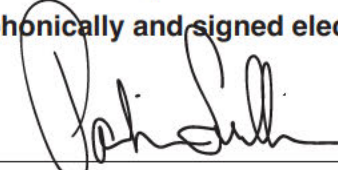


Federal Bureau of Investigation

Attested to by the applicant in accordance with the requirements of Fed.  
R. Crim. P. 4.1 by telephone. **Sworn telephonically and signed electronically**

July 29, 2021

*Date*

  
*Judge's signature*

Providence, RI

*City and State*

Patricia A. Sullivan, US Magistrate Judge

*Printed name and title*